

RECEIVED  
CENTRAL FAX CENTER

NOV 07 2006

Serial No. 10/027,622

Docket No. NG(MS)7194

**REMARKS**

Claims 1-16 are currently pending in the subject application, and are presently under consideration. Claims 1-16 are rejected. Favorable reconsideration of the application is requested in view of the comments herein.

**I. Rejection of Claims 1-6, 8-14 and 16 Under 35 U.S.C. §103(a)**

Claims 1-6, 8-14 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,192,131 to Geer, Jr. et al. ("Geer") in view of U.S. Patent No. 6,615,171 to Kanevsky et al. ("Kanevsky"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Regarding claims 1 and 9, Geer taken in view of Kanevsky does not teach or suggest accessing a token through a token reader connected to a computer system by a certificate authority, as recited in claims 1 and 9. In rejecting claims 1 and 9, the Examiner contends that Column 2, Lines 27-39 of Geer discloses this element of claims 1 and 9. Applicant's representative respectfully disagrees. The cited section of Geer discloses that a smart card at an authorizing computer 10 is initialized by the creation of a public key pair for the smart card and a public key pair for the user of the card (See Geer, Col. 2, Lines 40-45). The cited section of Geer also discloses that a certifying authority 18 performs the conventional function of certifying the identity of the user to authorized computer 14 and transaction computer 16 (See Geer, Col. 2, Lines 36-39).

The cited section of Geer does not teach or suggest that the certifying authority (i.e. certificate authority) can access the smart card (i.e. token) at authorizing computer 10. Instead, Geer discloses that a user is verified by authorizing computer 10 sending the authorized computer 14 an identification certificate signed with the private key of the certifying authority, and the authorized computer 14 verifies the authenticity of the signature on the identification certificate (See Geer, Col. 2, Lines 50-60). That is, in claims 1 and 9, the certificate authority access the token, while in Geer, identity is verified by passing the identification certificate from the authorizing computer 10 to the authorized computer 14, and to the certifying authority.

Serial No. 10/027,622

Docket No. NG(MS)7194

Accordingly, Geer taken in view of Kanevsky does not teach or suggest accessing a token through a token reader connected to a computer system by a certificate authority, as recited in claims 1 and 9.

Moreover, in rejecting claims 1 and 9, the Examiner contends that Geer discloses downloading a certificate and an associated private key to a token (See Office Action, Page 3, Citing Geer, Col. 6, Lines 15-27). Applicant's representative respectfully disagrees with this contention. The U.S. Court of Appeals for the Federal Circuit ("Federal Circuit") has held that the determination of obviousness requires an evaluation of the claimed invention *as a whole*, and not merely the differences between the claimed invention and the prior art (emphasis added). *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, 221 U.S.P.Q. 1025, 1033 (Fed. Cir. 1984). Applicant's representative respectfully submits that in rejecting claims 1 and 9, the Examiner is not considering claims 1 and 9, as a whole.

Specifically, when claims 1 and 9 are read as a whole, it is clear that the certificate that is downloaded to token is the same token from which a user-signature certificate is read. In rejecting claims 1 and 9, the Examiner contends Column 2, Lines 51-60 of Geer discloses reading a user-signature certificate from a token (See Office Action, Page 5). The cited section of Geer discloses that an authorizing computer 10 sends an authorized computer 14 a public key certificate (i.e. an identification certificate) identifying a user and the user's public key (See Geer, Col. 2, Lines 51-55). Assuming *arguendo* that an identification certificate is similar to a signature certificate, Geer still fails to teach or suggest the downloading recited in claims 1 and 9. The section of Geer that the Examiner contends discloses the downloading recited in claims 1 and 9, discloses that authorizing computer 10 sends an authorization certificate to a smart card at authorized computer 14 that interacts with a program stored at the authorized computer 14 (See Geer, Col. 6, Lines 7-10). That is, the smart card at authorized computer 14 is a different smart card than the smart card from which the identification certificate is provided. Geer does not teach or suggest that the smart card at the authorized computer 14 contains an identification certificate (i.e. a signature certificate).

Serial No. 10/027,622

Docket No. NG(MS)7194

While Geer does disclose that the authorized computer 14 sends a public key certificate to the authorizing computer 10 identifying the user of the authorized computer 14 (See Geer, Col. 2, Lines 60-63), Geer fails to teach or suggest that the public key certificate is ever stored on a smart card at the authorized computer 14. In fact, in the section of Geer that the Examiner contends discloses the downloading recited in claims 1 and 9 discloses that interaction with the smart card at the authorized computer 14 occurs when the authorized computer 14 contains a program that requires a license or a program fragment to function (See Geer, Col. 6, Lines 10-14). The cited section of Geer is not related to identification of the user of authorized computer 14. Thus, the sending of an authorization certificate to a smart card at authorization computer 14 does not correspond to the downloading recited in claims 1 and 9. Accordingly, Geer taken in view of Kanevsky does not teach or suggest downloading a certificate and an associated private key to a token, when claims 1 and 9 are read as a whole.

Additionally, Applicant's representative agrees that Geer does not teach or suggest searching for a token ID and a user signature certificate from a token, searching for a match for the token ID and the user signature certificate in an authoritative database and that a certificate and an associated private key are wrapped with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database, as recited in claims 1 and 9. In fact, Geer is silent on a smart card (i.e. a token) having a smart card ID (i.e. token ID). Additionally, in contrast to the contentions of the Examiner, the addition of Kanevsky does not make up for the deficiencies of Geer. In rejecting claims 1 and 9, the Examiner cites Col. 8, Lines 29-46 of Kanevsky. The cited section of Kanevsky discloses that if a user forgets his personal identification number (PIN) or if his PIN expires without being reset that the user can reestablish his PIN by linking to an automatic speech/speaker recognition (ASSR) server 200 via a communication link to request a PIN reset through a personal computer (PC) 450 and a smart card reader 460 (See Kanevsky, Col. 8, Lines 21-28). Kanevsky also discloses that a user provides his user ID, name and smart card serial number to the ASSR server 200 (See Kanevsky, Col. 8, Lines 31-34). Kanevsky further discloses that the ASSR server 200 accesses a stored certificate and the ASSR server 200 uses the smart card's certificates and public

Serial No. 10/027,622

Docket No. NG(MS)7194

key to encrypt a PIN reset command, which is activated by the smart card (See Col 8., Lines 35-47).

Kanevsky does not teach or suggest that a certificate and an associated private key are wrapped with a public key associated with a token ID, as recited in claims 1 and 9. Instead, Kanevsky discloses that a PIN reset command is encrypted with a smart card's certificate and public key. Clearly, the PIN reset command does not correspond to the certificate recited in claims 1 and 9. Accordingly, taken individually or in combination, Geer and Kanevsky do not teach or suggest each and every element of claims 1 and 9.

Furthermore, Applicant's representative respectfully submits that there is no motivation to combine and modify the teachings of Geer and Kanevsky in the manner suggested by the Examiner. Trade-offs concern what is feasible, while motivation to combine requires what is desirable. *Winner Int'l Royalty Corp. v. Ching-Rong Wang* 202 F.3d 1340, 1349 53 U.S.P.Q.2d 1580 (Fed. Cir. 2000). In *Winner*, the Federal Circuit held that one of ordinary skill in the art would not have reasonably elected trading the benefit of security for that of convenience. 202 F.3d 1340, 1349, 53 U.S.P.Q.2d 1580. As stated above, Geer does not even mention the employment of smart card IDs (i.e. token IDs). Applicant's representative respectfully submits that if the system disclosed in Geer were modified to employ smart card IDs in the manner suggested by the Examiner, particular smart cards (i.e. tokens) would need to be assigned to particular users and computers in an authoritative database. That is, the smart cards would not be generic or transferable (e.g. by copying contents of the smart card). There is no motivation in Geer to employ such a system, as employing smart card IDs (i.e. token IDs) would result in a less convenient system. One skilled in the art would not be motivated to tradeoff the benefit of using a generic smart card for the increased security and complexity of a system where the smart cards were assigned to particular users and computers. Thus, there is no motivation to combine and modify the teachings of Geer and Kanevsky in the manner suggested by the Examiner. Therefore, Geer taken in view of Kanevsky does not make claims 1 and 9 obvious, and claims 1 and 9 should be patentable over the cited art.

Serial No. 10/027,622

Docket No. NG(MS)7194

Claims 2-6, 8, 9-14 and 16 depend either directly or indirectly from claims 1 and 9, respectively, and are not obvious for at least the same reasons as claims 1 and 9, and for the specific elements recited therein. Accordingly, claims 2-6, 8, 9-14 and 16 should be patentable over the cited art.

Additionally, regarding claims 2 and 10, Geer taken in view Kanevsky, does not teach or suggest that a certificate and an associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy, as recited in claims 2 and 10. Claims 2 and 10 defines properties of the certificate recited in claims 1 and 9 that is downloaded to a token. In rejecting claims 2 and 10, the Examiner cites Col. 3, Lines 29-33 of Geer. Geer discloses that an authorization certificate is generated by a smart card on an authorizing computer 10 (See Geer, Col. 3, Lines 23-24) and the smart card signs the authorization certificate with the private key of the smart card (See Geer Col. 3, Lines 33-34). Geer also discloses that the authorizing computer 10 sends the authorization certificate to a smart card at authorized computer 14 (See Geer, Col. 6, Lines 8-10). However, since claims 2 and 10 depend from claims 1 and 9, respectively, the certificate recited in claims 2 and 10 is downloaded to the token, which is the same token from which a user signature certificate is read.

For the reasons stated above, Geer taken in view of Kanevsky does not teach or suggest reading a token ID and a user-signature certificate from a token and downloading a certificate and associated private key to the same token, as recited in claims 1 and 9, from which claims 2 and 10 depends. Therefore, Geer taken in view Kanevsky does not teach or suggest specific properties of the certificate that is downloaded to the token, as recited in claims 2 and 10. Thus, Geer taken in view of Kanevsky not teach or suggest each and every element of claims 2 and 10.

For the reasons described above, claims 1-6, 8-14 and 16 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

Serial No. 10/027,622

Docket No. NG(MS)7194

**II. Rejection of Claims 7 and 15 Under 35 U.S.C. §103(a)**

Claims 7 and 15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Geer and Kanevsky and further in view of U.S. Publication No. 2003/0005291 to Burn ("Burn"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 7 and 15 depend from claims 1 and 9, respectively. The further addition of Burn does not make up for the aforementioned deficiencies of Geer taken in view of Kanevsky, with respect to claims 1 and 9, from which claims 7 and 15 depend.

Additionally, Applicant's representative agrees that Geer taken in view of Kanevsky does not teach or suggest decrypting a certificate and associated private key using a private key stored in the token requires the entry of a passphrase by a user, as recited in claims 7 and 15. Applicant's representative respectfully submits that Geer, Kanevsky and Burn teach away from their respective combination and modification in the manner suggested by the Examiner. The Federal Circuit has held that references teach away from their combination if the references taken in combination would produce a seemingly inoperable device. *McGinley v. Franklin Sports Inc.*, 262 F.3d 1339, 1354, 60 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 2001). In Kanevsky, the only reasons taught or suggested for sending a PIN reset command, as discussed above with respect to claims 1 and 9, is when a user forgets his PIN or the PIN has expired (See Kanevsky, Col. 8, Lines 21-23). Accordingly, a user in such a situation would not be able to enter a PIN, as either the user would not know the PIN, or the PIN would be expired. In contrast, claims 7 and 15 require that a passphrase be entered by a user. If the teachings of Geer and Kanevsky were combined and modified with Burn such that a user were required to enter a PIN when the user forgot his PIN or the PIN were expired, the user would not be able to decrypt the PIN reset command, since that user would not be able to remember his PIN, or the PIN would no longer be valid (i.e., expired).

In the Office Action, the Examiner contends that Kanevsky discloses several reasons for sending the PIN reset command (See Office Action, Page 4, citing Col. 8, Lines 21-31). However, the cited section of Kanevsky only discloses the two reasons discussed above, namely, if the user forgot his PIN or if the PIN has expired without resetting. As stated above, in either

Serial No. 10/027,622

Docket No. NG(MS)7194

case, the user would not be able to decrypt the PIN reset command. Accordingly, Applicant's representative respectfully submits that combining and modifying the teachings of Geer, Kanevsky and Burn in the manner suggested by the Examiner would result in an inoperable device, and thus, the references teach away from their combination.

For the reasons described above, claims 7 and 15 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

RECEIVED  
CENTRAL FAX CENTER

NOV 07 2006

Serial No. 10/027,622

Docket No. NG(MS)7194


CONCLUSION

In view of the foregoing remarks, Applicant's representative respectfully submits that the present application is in condition for allowance. Applicant's representative respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date:

11-7-06  
\_\_\_\_\_  
Christopher P. Harris  
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.  
1300 EAST NINTH STREET, SUITE 1700  
CLEVELAND, OHIO 44114  
Phone: (216) 621-2234  
Fax: (216) 621-4072